PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-287192
(43)Date of publication of application : 13.10.2000

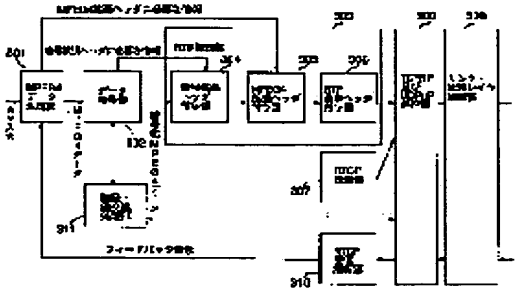
(51)Int.Cl. H04N 7/167
G09C 1/00
H04L 9/08
H04L 9/32
H04L 12/56

(21)Application number : 11-093916
(22)Date of filing : 31.03.1999

(71)Applicant : TOSHIBA CORP
(72)Inventor : SAITO TAKESHI
KATO HIROSHI
TOMOTA ICHIRO
TAKAHATA YOSHIAKI
AMI JUNKO

(54) INFORMATION DISTRIBUTING DEVICE, RECEIVING DEVICE AND COMMUNICATION METHOD

(57)Abstract:
PROBLEM TO BE SOLVED: To extend copy protection technique to a digital contents circulation by executing a transport protocol processing required for transferring contents information, creating a basic transport header which indicates that contents information is enciphered and transmitting a packet including desired information to a communication opposite party by way of a network.
SOLUTION: MPEG4 data outputted from an MPEG4 data creating part 301 are enciphered by a data enciphering part 302. An authentication and key exchange processing part 311 generates a new cipher key for an enciphering processing in the case of the updating timing of the cipher key and gives it to the data enciphering part 302. Together with it, the value of information to be a source for generating a common key is increased and given to the part 302. The value of information to be the source for generating the common key is given from the part 302 to a cipher extension header giving part 304. An MPEG4 extending header is exempted from a ciphering object.



LEGAL STATUS

[Date of request for examination] 19.03.2002

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

[0029]

[Embodiments of the Present Invention] Below, the present embodiments of the invention will be presented with reference to figures.

[0030] (First embodiment) In FIG.1, the information distribution system in the present embodiment is shown. In FIG.1, an MPEG4 distribution server 101 and a receiving device 102 according to the present embodiment are connected by an internet 103, and confidential communication of an MPEG4 AV stream is performed over the internet between MPEG4 distribution server 101 and receiving device 102. Of course it does not matter whether another MPEG4 distribution server and receiving device, or other types of hardware, are connected to internet 103.

[0031] Likewise, although the data type for the present embodiment is described as MPEG4, the present invention is of course applicable to other types of data.

[0032] MPEG4 distribution server 101 delivers MPEG4 data to receiving device 102. The MPEG4 data takes the form of stream distribution, not file transfer. At this time, the MPEG4 data targeted for copyright protection is delivered in an encrypted state. At this time prior to distribution, the authentication procedure and the exchange of authentication keys are carried out between MPEG4 distribution server 101 and receiving device 102.

[0033] An example of the sequence for this is shown in FIG.2.

[0034] Note that FIG.2 is a display of the encryption and authentication of what is called a content layer and also that security in a layer such as an IP layer or a transport layer, as well as the authentication and so on, for these layers are omitted. Likewise, procedures such as accounting that are performed ahead in the content layer are also omitted (there may be cases where accounting processing and authentication/encryption procedures are not carried out).

[0035] Here a case where receiving device 102 requests distribution from the MPEG4 distribution server 101 is considered. In this case, the first authentication request is sent out from the receiving device 102 (S201). In the authentication request, it is also possible to simultaneously perform an exchange of a certification (certificate, device certification) that such device (receiving device 102) has received, from a pre-determined authentication institution, an authentication that is "a device capable of performing an exchange of copyright-protected contents".

[0036] Here an IP address may be used for the "device ID" utilized at the time of device certification but in the case where the IP address is assigned by the DHCP server, there is a possibility that the device ID will become a variable value each time the device boots. Therefore, the MAC address of the device or the EU164 address

or something that has assigned a part module number to those addresses can be used for the device ID used in device certification. Likewise, the identification number of the CPU of that device and the identification number of the MPEG4 decoder and so on can be used as if (ideally) they were a globally unique figure (or unique in a region and so on, a value that is not expected to have a value identical to it for the most part).

[0037] MPEG4 distribution server 101, which received a message from receiving device 102, carries out a response to the authentication request and exchanges certificates (device certification) (S202).

[0038] Next, MPEG4 distribution server 101 and receiving device 102 perform a generation process for a certification key in order to generate a common certification key (S203). The specifics of this procedure can be the same as for example a generation process for a certification key for copy protection for IEEE1394. When the process finishes, MPEG distribution server 101 and receiving device 102 can share common Kauth authentication keys without a third party knowing.

[0039] Next, MPEG4 distribution server 101 transmits exchange key Kx, authentication key Kauth, their exclusive disjunction XOR (Kx EX-OR Kauth) and random number Nc to receiving device 102 (S204, S205). In receiving device 102, the received value and (Kauth) value and the XOR are calculated (Kx EX-OR Kauth EX-OR Kauth=Kx) and exchange key Kx is derived.

[0040] At this point, MPEG4 distribution server 101 and receiving device 102 are sharing three types of figures: authentication key Kauth, exchange key Kx and random number Nc.

[0041] Here, encryption key (contents key) Kc, i.e. the encryption key for encrypting MPEG4 data that MPEG4 distribution server 101 must transmit, and the encryption key (common key) Kc for de-encrypting encrypted MPEG 4 data received by receiving device 102, is calculated in each MPEG distribution server 101 and each receiving device 102 as a function of one part of the above values, by utilizing the same pre-determined function J. For example, it is calculated that Kc=J [Kx, f(EMI), Nc]. Here, EMI stands for "the copy attribute of the data (contents)", and it expresses the attribute of "whether that data can be copied unlimitedly, can be copied only once or twice, can be copied unconditionally or whether once it is copied, it cannot be copied again,…" and so on. This attribute value EMI transformed in a specific function f is f(EMI). These functions J and f can be secret from the outside.

[0042] After encryption key Kc has been generated, MPEG4 distribution server 101 encrypts a contents (MPEG4 data) with the encryption key Kc and transfers it over

the internet (S206, S207,···).

[0043] Note that as mentioned below, since the encrypted contents more and more take the form of a "real-time transfer of AV stream data" and are transferred over the internet, an RTP (Real-time Transport Protocol) is employed as a transport protocol.

[0044] Likewise, this encryption key Kc is assumed to be time-variable (i.e., as time elapses the value changes). For example, when it is recognized that time has lapsed from a time of the previous change to a given time (the given time can be fixed or adjustable), the value of the variable number Nc is incremented and the value of encryption key Kc is calculated again using the above function J. At this time, it is necessary that the timing that updates the encrypted Kc value (or the data that encryption key Kc updates from) is synchronized and recognized on the transmitting side. Thus, an Even/Odd field range is created in the transferred MPEG4 data (AV data) that prescribes the turning point of the field's value as the turning point of the value of variable number Nc and by extension the turning point of encryption key Kc's value (the post-update encryption key Kc is applied from the data).

[0045] In other words, the encryption key Kc monitors an elapsing of the time above in MPEG4 distribution server 101, and in the case where it is detected that the time has become the timing that updates encryption key Kc, the value of variable number Nc is incremented and the value of encryption key Kc is re-calculated. Along with encrypting the MPEG4 data that must be sent using the encryption key Kc after re-calculation, the value of the Even/Odd field is incremented and transmission is performed. Afterwards, encryption is performed using the encrypted key Kc until the next update timing. On the other hand in receiving device 102, the received Even/Odd field value is monitored and in the case where it is detected that the value of the field is incrementing compared to the value immediately before reception, the value of variable number Nc is incremented, the value of encryption key Kc is re-calculated and the encrypted data is decrypted using the encryption key Kc after re-calculation. Afterwards, decryption is performed with this encryption key Kc until a change in the value of the Even/Odd field is next detected.

[0046] In this way, encrypted MPEG4 data is exchanged between MPEG4 distribution server 101 and receiving device 102.

[0047] In FIG.3, an example of an internal structure of an MPEG4 distribution server is shown.

[0048] As shown in FIG.3, the MPEG4 distribution server 101 in the present embodiment comprises an MPEG4 generation unit 301, a data encryption unit 302, an

RTP processing unit 303 which carries out RTP processing and includes an encryption expansion header attachment unit 304, an MPEG4 expansion header attachment unit 305 and an RTP base header attachment 306; an RTCP transmission unit 307, a TCP/IP and UDP/IP processing unit 308, a link/physical layer processing unit 309, an RTCP reception analysis unit 310 and an authentication/key exchange processing unit 311.

[0049] A process related to sequence authentication and encryption (the process from S201-S205) as well as a process related to encryption key renewal is performed by the authentication/key exchange processing unit 311.

[0050] The inputted AV input (for example an analog signal) is compressed into MPEG4 data in the MPEG4 data generation unit.

[0051] At this time, the receiving side is notified of the attribute information concerning the generating MPEG4 such as where the I picture is located and what the encryption rate is, and playback (decryption) processing on the receiving side may become easier to perform. Because rejections, delays, changes in arrival order and so on of transferred packets may occur, especially over the internet, obtaining attribute information is indispensable for playback at high quality on the receiving side. For example, for the MPEG4 in the present embodiment, the information related to the VOP header and so on corresponds to the attribute information of the MPEG4. Also there may be cases where information concerning the MPEG4 system is needed, for example synchronization information transferred by a Sync Layer and the information for multiplexing for transmitting multiplexed pluralities of MPEG4 streams, or information related to the initial value of an object descriptor and its latest value and so on. Therefore, in the case where AV data is transferred at RTP, attribute data is sent in parallel with AV data in the form of the RTP expansion header or a payload header for an RTP payload.

[0052] In the present embodiment, it is supposed that the attribute information is sent in the form of an RTP expansion header. In other words, the attribute information is sent as an "MPEG4 expansion header" type (ID) RTP expansion header. Thus, the necessary information is communicated from MPEG4 data generation unit 301 to MPEG 4 header attachment unit 305.

[0053] Next, the MPEG4 data outputted from MPEG4 data generation unit 301 is encrypted by data encryption unit 302. At that time the encryption key used is the time-variable encryption key Kc mentioned above. Also, a diversity of attribute information is possible regarding the encryption process, and in the present embodiment, the "encryption expansion header" type (ID) RTP expansion header is

attached at encryption expansion header attachment unit 304. As a result, encryption expansion header attachment unit 304 is notified from data encryption unit 302 of necessary information.

[0054] Note that in the case where the update timing of encryption key Kc has been reached in the authentication/key exchange processing unit 311, Nc is incremented and a new encryption key Kc is generated for the encryption process above by function J and given to data encryption unit 302. Together with this also the value of the Even/Odd field is incremented and given to data encryption unit 302. The value of the Even/Odd field is transmitted as above from the data encryption unit 302 to the encryption expansion header attachment unit 304.

[0055] Here in FIG.4, an example of an encryption expansion header is shown. As shown in FIG.4, there is an expansion header type field, a with-or-without encryption field, an encryption format display field, an encryption mode indicator field (EMI) and an Even/Odd field in this encryption expansion header. The expansion header type field is a field for describing information that indicates the type of the expansion header. Here, information that indicates an encryption expansion header is described inside the expansion header type field. The with-or-without encryption field is a field for describing information that indicates whether transferred information in the RTP packet is encrypted or not. The encryption format display field is a field for describing information that indicates the encryption format used in data sent in the RTP packet. For example, information indicating that the encryption format is M6 is described. The encryption mode indicator field (EMI) is a field for describing the copy attribute value EMI. The Even/Odd field is a field, as indicated above, for notifying the receiving side of the encryption key update timing from the transmitting side.

[0056] Note that here, each field is assumed for example to be 8 bits but this is not restricted; it is possible to determine this as appropriate.

[0057] Here, when encrypting AV data and transmitting it to the receiving side, processing may become difficult on the receiving side in the case where the still images are being sent in parts or using trick play such as fast forward and so on. This follows from the difficulties in transmitting only one part of the encrypted AV stream (for reasons such as the Nc value not being incremented, and instead increasing sharply for instance). Thus in a certain situation there may be instances where AV data is sent to the receiving side without encryption. In this situation, there needs to be a mechanism to notify the receiving side of the information that "this AV data is encrypted/is not encrypted". The with-or-without encryption field

above is used for this purpose for instance.

[0058] Also, it is possible that different encryption methods co-exist on the internet, such that "this encryption method is used for a stream and this encryption method is used for another stream". In this kind of situation, in the case where there is a field that indicates "which encryption method is this AV data encrypted by?" the receiving side sees this, selects an appropriate decryption engine and becomes able to decrypt the code. The encryption format display field above is for instance used for this purpose.

[0059] Also, as shown in FIG.4, the encryption mode indicator (EMI) field is set to 8 bits, unlike the 2 bits in the case of IEEE1394. This is done so a case where information is notified to the receiving side that "this AV data can be copied N number of times" can be adapted to by setting degrees of freedom for the numerical value N selection and by setting the value of this field to take many values in the case of permitting a particular kind of copy (for example when copying is only possible if certain conditions are fulfilled) and so on.

[0060] Also as shown in FIG.4, 8 bits is set in the Even/Odd field, differing from IEEE1394 by 1 bit. This is done because packet rejection, delay and arrival order changeovers may occur on the internet, and out of concern that the amount of information in 1 bit is not sufficient. In other words, it could be assumed that, as shown in S207, all packets with an Even/Odd field=1 will be rejected on the internet. In this case where the Even/Odd field is set to 1 bit, the receiving side will recognize that "the Even/Odd=0 state is continuing (no change in Even/Odd bit)" since the Even/Odd bit will return to 0 in the next packet. Thus there may be a problem that even though Nc should actually be incremented by 2, the Nc value won't be incremented and the correct encryption key cannot be generated because the receiving side will recognize that the Even/Odd bit value is not changing. Thus, the Even/Odd field is set to more than 2 bits, for example 8 bits, so that even in the case where packet rejection/delay/arrival order changeovers occur, the receiving side is prepared to implement the appropriate process.

[0061] Here in the present embodiment, data encryption is only implemented for the MPEG4 data itself and is not implemented for MPEG4 expansion headers. Since MPEG4 expansion headers are not used for what is called "contents that must be copy-protected", but instead to use the MPEG4 data itself in advance on the receiving side, MPEG4 expansion headers are not an object for encryption.

[0062] Ultimately, the encryption expansion header is attached to encryption expansion header attachment unit 304, the MPEG4 expansion header to MPEG4

expansion header attachment unit 305, the RTP base header to RTP base header attachment unit 306 and the RTP header form is attached as shown in FIG.5. Here, the encryption expansion header is generated based on information from data encryption unit 302 and the MPEG4 expansion header is generated based on information from MPEG4 data generation unit 301. Also, the RTP header possesses as components the basic parameters such as timestamp and sequence number that are necessary for transferring AV data over the internet (note that specifics are disclosed in RFC1889 for instance).

[0063] The (encrypted) MPEG 4 data attached to the RTP header is transmitted at TCP/IP and UDP/IDP processing unit 308 by internet 103 through link/physical layer processing unit 309 as an IP packet, as in FIG.6.

[0064] In FIG.7 the interior configuration of receiving device 102 is shown.

[0065] As shown in FIG.7, the MPEG4 distribution server 101 in the present embodiment comprises a link/physical layer processing unit 701, a TCP/IP and UDP/IP processing unit 702, an RTP processing unit 703 which performs RTP processing and includes an RTP base header reception analysis unit 704, an MPEG4 expansion header analysis unit 705 and an encryption expansion header reception analysis unit 706; a data encryption-decryption unit 707, an MPEG 4 data decoding unit 708, a reception state analysis unit 709, an RTCP transmission unit 710 and an authentication/key exchange processing unit 711.

[0066] The process related to sequence recognition and encryption (the process from S201-S205) in FIG.2 as well as the process related to encryption key updating are performed by authentication/key exchange processing unit 711.

[0067] Reception device 102 basically performs the inverse transformation processes of MPEG4 distribution server 101 in inverse order.

[0068] In other words first, the MPEG4 data transferred through internet 103 (the encrypted data with RTP header attached) passes TCP/IP and UDP/IP processing unit 702 from link/physical layer processing unit 701 and is inputted into RTP processing unit 703.

[0069] In RTP processing unit 303, the RTP base header is analyzed at the RTP base header analysis unit 704, the MPEG4 expansion header is analyzed at MPEG4 expansion header reception analysis unit 705 and the encryption expansion header is analyzed at encryption expansion header reception analysis unit 304. Likewise, MPEG4 data decoding unit 708 is notified of necessary information from MPEG4 expansion header reception analysis unit 705, and data encryption-decryption unit 707 is notified of necessary information from encryption expansion header reception

analysis unit 304.

[0070] Then encrypted RTP payload data is passed from RTP processing unit 703 to data encryption-decryption unit 707. Data encryption-decryption unit 707 performs decryption (breaks the code) based on information from encryption expansion header reception analysis unit 304.

[0071] The time-variable encryption key Kc is the encryption key at this time. More specifically, data encryption-decryption unit 707 ascertains that the received data is encrypted (and as a result, it is determined that the unit must perform decryption) by referencing the value of the with-or-without encryption field of the encryption expansion header notified from encryption expansion header reception analysis unit 304; next it references the Even/Odd field and by comparing that value to the value received just before, it ascertains that the encryption key must be updated in the case where the Even/Odd field value is incrementing (when the values are the same, the encryption key will not be renewed). Next, instructions to renew the encryption key are communicated to authentication/key exchange processing unit 711 from data encryption-decryption unit 707 and since the update timing of encryption key Kc has been reached, Nc increments and a new encryption key Kc is generated from function J and is passed to data encryption-decryption unit 707.

[0072] Further, decrypted (decoded) MPEG 4 data is passed from data encryption-decryption unit 707 to MPEG4 data decoding unit 708 which decodes the MPEG4 data in question based on information from MPEG4 expansion header reception analysis unit 705 and the data is outputted as AV output (for example, an analog signal).

[0073] Incidentally an RTCP protocol (Real-time Transport Control Protocol) accompanies the RTP. This RTCP monitors the RTP sequence number, the timestamp and so on and has a function that notifies the transmitting side (for the present embodiment, MPEG4 distribution server 101) of the reception status (such as packet rejection rate and packet distribution delay times) from the receiving side (for the present embodiment, receiving device 102). A reception status analysis unit 709 of receiving device 102 and RTCP transmission unit 710 perform this function. MPEG distribution server 101 receives this RTCP packet in RTCP reception analysis unit 310 and optimization can be performed by giving feedback to MPEG4 data generation unit 301 according to necessity. For instance when packet rejections are heavy and it is considered that the network is congested, feedback control such as reducing the MPEG4 data generation bit rate, can be carried out. Note that the RTCP transmission unit 307 transmits necessary information for RTCP to the MPEG4

distribution server 101.

[0074] Next, as mentioned above, the value of variable number Nc which is used for the calculation of encryption key Kc changes based on the observation of the Even/Odd field that is included in the encryption expansion header of the reception packet. Consequently, in the case where it cannot reliably be communicated that the Nc value has been updated, it will not be possible to measure the value of encryption key Kc on the receiving side and it will become impossible to decrypt incoming encrypted data.

[0075] Because the internet is basically a network where packet rejections may occur, there is no guarantee that the meaning of the value of the Even/Odd field (the timing of the increment) will be communicated to the communications peer (especially when the bit length of the Even/Odd field is low). Thus, there may be an option for requesting the Nc value from a transmitting device (in the present embodiment, MPEG4 distribution server 101) prepared for the case where receiving device 102 ascertains the correct Nc value.

[0076] Here, in order for receiving device 102 to know the correct Nc value, in the case where there is a higher-than-assumed "jump" in the value of the timestamp of the RTP base header or in the sequence number and so on, a method of transmitting the packet requesting the Nc value to the transmitting side is conceivable. This "higher-than-assumed jump in the value" connects to the fact that "in the interval, there is a possibility that the value of the Even/Odd bits has changed". The units that perform these processes are the MPEG4 distribution server or the authentication/key exchange processing unit of reception device 102. This way, even supposing that the synchronization of MPEG4 server 101 and receiving device 102 were off, it would be possible to implement an appropriate recovery process. Note that, in the case where receiving device 102 is notified of the Nc value from MPEG4 distribution server 101, the values of the timestamp and sequence number and so on, of the corresponding RTP and expansion header, payload header and so on, may also be set to notify simultaneously.

[0077] Additionally, delivered data may also be accumulated in a receiving device (or in other storage media such as a DVD-RAM installed in a receiving device). In this case, the delivered data may be accumulated, still encrypted, together with the corresponding encryption key Kc.

[0078] (Second embodiment) Next, a variation in the packet format of the first embodiment is presented as the second embodiment. Since the present embodiment is the same in structure and in function as the first embodiment, points

differing in the present embodiment from the first embodiment will be presented centrally.

[0079] In the first embodiment, the "encryption expansion header" and the "MPEG4 expansion header" were attached as an expansion header of the RTP header (see FIG.5, FIG.6), in the present embodiment an "encryption expansion header" is attached as an expansion header of an RTP header and an "MPEG4 expansion header" is installed as a payload header to an RTP payload (see FIG.9, FIG.10); these are some points differing in the present embodiment from the first embodiment.

[0080] The overall structure of the network in the present embodiment is the same as the first embodiment (FIG.1). The processing sequence is also the same as the first embodiment (FIG.2). The encryption expansion header is also the same as the first embodiment (FIG.4).

[0081] An example of the structure of the MPEG4 distribution server 101 in the present embodiment is shown in FIG.8. A point of difference between the present embodiment and the first embodiment is that the process of the MPEG4 expansion header falls outside of the RTP process, since the MPEG4 expansion header is installed as a payload header on the RTP payload and so the MPEG4 expansion header attachment unit 305 of FIG.3 is expelled from inside RTP processing unit 303, becoming MPEG4 payload header attachment unit 315.

[0082] In the present embodiment, the format of the RTP header utilized when encrypted AV data is sent is shown in FIG.9. Here, a "payload type" field is prepared which shows "the properties of the data transmitted in a corresponding RTP packet (coding method and such)". In the present embodiment in the case where for example the data transmitted is an encrypted MPEG4, information that indicates an "encrypted MPEG4" will be described. Receiving device 102 can ascertain whether or not the transmitted data is an encrypted MPEG4 or not by referencing this field. Also, in the present embodiment, an "X bit" field is prepared in the RTP base header that indicates "whether or not an expansion header is attached to the RTP header in question". In the present embodiment a bit is set indicating that "there is an expansion header".

[0083] The format of the whole IP packet transmitted over the internet in the present embodiment is shown in FIG.10.

[0084] An example of the structure of receiving device 102 in the present embodiment is shown in FIG.11. Differing from the first embodiment in the same way as the MPEG4 distribution server 101 above is that the process of the MPEG4 expansion header falls outside the RTP process and the MPEG4 expansion header reception

analysis unit 705 of FIG.7 is expelled from RTP processing unit 703, becoming MPEG4 payload header reception analysis unit 715.

[0085] At the RTP base header reception analysis unit 704 in receiving device 102 it is ascertained that the data received is an encrypted MPEG4, and also that an expansion header is attached to an RTP header. Then at encryption expansion header reception analysis unit 706, it is ascertained that the expansion header is an encryption expansion header and also that the encryption format, the presence or absence of an update of the encryption key and so on can be ascertained from the encryption expansion header. Like the first embodiment, the encrypted MPEG4 data is decrypted at data encryption-decryption unit 707, the MPEG4 payload header is analyzed at MPEG4 payload header reception analysis unit 715, and further, like the first embodiment, the MPEG4 data is decoded based on the above analysis results at MPEG4 data generation unit 708, then outputted as AV output (for example, an analog signal).

[0086] Note that in the present embodiment, in the case where information is described in the payload type field that includes a notification that there is encryption, the with-or-without encryption field in the encryption expansion header need not be referenced, and in the case where information is described in the payload type field that includes a notification that there is encryption, since this is a notification that the information is possibly encrypted, the encryption expansion header can be set to make the final decision as to the presence or absence of encryption according to the with-or-without encryption field.

[0087] (Third embodiment) Next the third embodiment will be presented. Differences between the present embodiment and the second embodiment will be presented centrally.

[0088] The format of an RTP header utilized when transmitting encrypted AV data in the present embodiment is shown in FIG.12. Also, the overall format of an IP packet transmitted over the internet in the present embodiment is shown in FIG.13.

[0089] Namely, in the second embodiment, whereas information including notification of the presence or absence of encryption or the possibility of its presence or absence such as "encrypted MPEG4", is described in the payload type field inside the RTP base header, in the present embodiment only "MPEG4" is described; there is no information described in the payload type field that includes notification of the presence or absence of encryption or the possibility of its presence or absence.

[0090] Therefore, in the present embodiment, receiving device 102 can ascertain that a received data is an MPEG4 by referencing the payload type field and the presence

or absence of encryption is recognized by referencing an RTP expansion header (encryption expansion header) of an RTP header.

[0091] At the RTP base header reception analysis unit 704 in receiving device 102, it is ascertained that the received data is an MPEG4 and also, that an RTP header is attached. At encryption expansion header reception analysis unit 706, it is then ascertained that the expansion header is an encryption expansion header and the presence or absence of encryption and the presence or absence of an update to the encryption key and so on can be ascertained from the encryption expansion header. Afterward is the same as the second embodiment.

[0092](Fourth embodiment) Next the fourth embodiment will be presented. Differences between the present embodiment and the second embodiment will be presented centrally.

[0093] In the second embodiment, the "encryption expansion header" is attached as an expansion header of the RTP header and the "MPEG4 expansion header" is installed as a payload header to the RTP payload but (see FIG.9, FIG.10) the difference with the present embodiment is that the "encryption expansion header" and the "MPEG4 expansion header" are both installed as a payload header to the RTP payload (see FIG.15, FIG.16).

[0094] The overall structure of the network in the present embodiment is the same as the second (first) embodiment (FIG.1). The processing sequence is also the same as the second (first) embodiment (FIG.2). The encryption expansion header (encryption payload header) is also the same as the second (first) embodiment (FIG.4).

[0095] An example of the structure of MPEG4 delivery server 101 in the present embodiment is shown in FIG.14. In the present embodiment, an encryption expansion header is added to an MPEG4 expansion header and is also installed to an RTP payload as a payload header and so the processing of the encryption expansion header falls outside of the RTP process, and also encryption expansion header attachment unit 304 is expelled from RTP processing unit 303, becoming encryption payload header attachment unit 314; this is a difference from the second embodiment.

[0096] In the present embodiment, the format of the RTP header utilized when encrypted AV data is sent is shown in FIG.15. The payload type field is the same as in the second embodiment. The function of the X bit field is also the same as in the second embodiment but in the present embodiment, a bit is set that indicates "no expansion header".

[0097] The whole format of the IP packet transferred over the internet in the present embodiment is shown in FIG.16.

[0098] An example of the structure of receiving device 102 is shown in FIG.17. Differing from the first embodiment in the same way as the MPEG4 distribution server 101 above, the processes of the MPEG4 expansion header fall outside the RTP process and the encryption expansion header reception analysis unit 706 of FIG.11 is expelled from RTP processing unit 703, becoming encryption payload header reception analysis unit 716.

[0099] At the RTP base header reception analysis unit 704 in receiving device 102, it is ascertained that the data received is an encrypted MPEG4, and likewise that an expansion header is not attached to an RTP header. In the present embodiment afterwards, subsequent processes are intended for the payload. First, at encryption payload reception analysis unit 716, it is ascertained that the payload header is an encryption expansion header and also, the encryption format, the presence or absence of an update to the encryption key and so on can be ascertained from the encryption payload header. Subsequently, like the second embodiment, the encrypted MPEG4 data is decrypted at encryption-decryption unit 707, the MPEG4 payload header is analyzed at MPEG4 payload header reception analysis unit 715, and further, the MPEG4 data is decoded based on the above analysis results at MPEG4 data generation unit 708, then outputted as AV output (for example, an analog signal).

[0100] Note that, in the present embodiment as in the second embodiment, in the case where information that includes a notification that there is encryption is described in the payload type field, the with-or-without encryption field in the encryption expansion center need not be referenced, and in the case where information is described in the payload type field that includes a notification that there is encryption, since this is a notification that the data is possibly encrypted, the final decision as to the presence or absence of encryption can be set to depend on the with-or-without encryption field of the encryption expansion header.

[0101] (Fifth embodiment) Next the fifth embodiment will be introduced. Differences between the present embodiment and the second embodiment will be presented centrally.

[0102] The format of an RTP header utilized when transmitting encrypted AV data in the present embodiment is shown in FIG.18. Also, in FIG.19, the format of an encryption expansion header is shown. Likewise, in the present embodiment, the whole format of an IP packet transmitted over the internet is shown in FIG.20.

[0103] In other words, in the second embodiment where information, including attributes of the encrypted data (its encoding format and so on) such as "encrypted MPEG4", is described in the payload type field inside the RTP base header (see FIG.9,

FIG.11); in the present embodiment, only information that notifies that encryption is present such as "encrypted data" is included in the payload type field (see FIG.18, FIG. 20). Subsequently, the encryption expansion header is attached as an expansion header of an RTP header and an MPEG4 expansion header is installed as a payload header to the RTP payload, in the same way as the second embodiment; but in the present embodiment, the properties of the above encrypted data (encoding format and so on) are described in the encryption expansion header (see FIG.4, FIG. 19).

[0104] The overall structure of the network in the present embodiment is the same as the second (first) embodiment (FIG.1). The processing sequence is also the same as the second (first) embodiment (FIG.2). Also, the MPEG4 distribution server and the interior structure of receiving device 102 are the same as the second embodiment (FIG.8, FIG.11).

[0105] In the present embodiment, a value is described in the payload type field of the RTP base header that indicates "encrypted data", as shown in FIG.18. Receiving device 102 ascertains that the transmitted data is encrypted data by referencing this field. In the present embodiment, a bit is set in the X bit field indicating that "an expansion header is present".

[0106] In the present embodiment, a payload type field is prepared for the encryption expansion header, as shown in FIG.19. In the payload type field information is described that indicates the type of data that enters the payload (for the present embodiment, MPEG4). Receiving device 102 can ascertain the type of data transmitted by referencing this field.

[0107] At the RTP base header reception analysis unit 704 in receiving device 102 it is ascertained that the data received is encrypted, and likewise, that an expansion header is attached to an RTP header. Subsequently, at encryption expansion header reception analysis unit 706, it is ascertained that the expansion header is an encryption expansion header and also that, the encryption format, the presence or absence of an update to the encryption key, the type of data that enters the payload and so on can be ascertained from the encryption expansion header. Then, like the second embodiment, the encrypted MPEG4 data is decrypted at encryption-decryption unit 707, the MPEG4 payload header is analyzed at MPEG4 payload header reception analysis unit 715, and further, the MPEG4 data is decoded based on the above analysis results at MPEG4 data generation unit 708, then outputted as AV output (for example, an analog signal).

[0108] Note that, in the present embodiment, in the case where information is described in the payload type field of the RTP base header indicating that there is

encryption, the with-or-without encryption field in the encryption expansion header need not be referenced, and if there is information described in the payload type field of the RTP base header which indicates encrypted data, since this is a notification that the data is possibly encrypted, the final decision as to the presence or absence of encryption can be made dependent on the with-or-without encryption field in the encryption expansion header.

[0109] (Sixth embodiment) Next the sixth embodiment will be presented. Differences between the present embodiment and the fourth embodiment will be presented centrally.

[0110] The format of the RTP header utilized when transmitting encrypted AV data in the present embodiment is shown in FIG.21. Also, the format of the encryption expansion header in the present embodiment is the same as in FIG.19. Likewise, in the present embodiment, the whole format of the IP packet transmitted over the internet is shown in FIG.22.

[0111] In other words, both the "encryption expansion header" and the "MPEG4 expansion header" installed as a payload header to the RTP payload are the same as in the fourth embodiment, (see FIG.15, FIG.16) but in contrast to the fourth embodiment where information is described in the payload type field in the RTP base header which includes notification of the characteristics of the encrypted data (encoding format and so on) like "encrypted MPEG4", in the present embodiment only information that notifies the receiving side that encrypted data is present, such as "encrypted data", is described in the payload type field (see FIG. 21, FIG.22). Subsequently, the attachment of the encryption expansion header as the expansion header of the RTP header and the installation of the MPEG4 expansion header as a payload header to the RTP payload is the same as in the second embodiment, but in the present embodiment, the characteristics of the above encrypted data (encoding method and so on) are described inside the encryption expansion header (see FIG.4, FIG. 19).

[0112] The overall structure of the network in the present embodiment is the same as the fourth (first) embodiment (FIG.1). The processing sequence is also the same as the fourth (first) embodiment (FIG.2). Also, the MPEG4 distribution server and the interior structure of receiving device 102 are the same as the fourth embodiment (FIG.14, FIG.17).

[0113] In the present embodiment, a value enters into the payload type field of the RTP base header that indicates "encrypted data", as shown in FIG.21. Receiving device 102 ascertains that the transmitted data is encrypted by seeing this field.

Also, a bit is set in the X bit indicating that "an expansion header is absent". Also, as in the fourth embodiment, information that describes the type of data (for the present embodiment, MPEG4) that enters the payload is described in the payload type field of the encryption expansion header.

[0114] At the RTP base header reception analysis unit 704 in receiving device 102 it is ascertained that the data received is encrypted, and likewise, that an expansion header is not attached to the RTP header. In the present embodiment the following becomes the process for the payload. First, at encryption payload reception analysis unit 716, it is ascertained that the payload header is an encryption expansion header and also that the encryption format, the presence or absence of an update to the encryption key and so on can be ascertained from the encryption payload header. Then, the encrypted MPEG4 data is decrypted at encryption-decryption unit 707, the MPEG4 payload header is analyzed at MPEG4 payload header reception analysis unit 715, and further, the MPEG4 data is decoded based on the above analysis results at MPEG4 data generation unit 708, then outputted as AV output (for example, an analog signal) as in the fourth embodiment.

[0115] Note that in the present embodiment as in the fourth embodiment, in the case where information is described in the payload type field of the RTP base header that indicates encrypted data, the with-or-without encryption field in the encryption expansion center need not be referenced, and in the case where information is described in the payload type field that indicates encryption, since this is a notification indicating that the data is possibly encrypted, the final decision as to the presence or absence of encryption can be set to depend on the with-or-without encryption field of the encryption expansion header.

[0116](Seventh embodiment) In the first through sixth embodiments, the invention was presented for the case that it was applied to a system that uses RTP as a transport protocol, but the invention is also compatible with systems that use other protocols.

[0117] In the seventh embodiment, an example case is presented of performing MPEG4 data distribution without using RTP as a transport protocol and instead using HTTP (Hyper-text Transfer Protocol) (and TCP), a protocol between a WWW server and a web browser.

[0118] An example structure of an information distribution system in the present embodiment is shown in FIG. 23. In FIG.23, an MPEG4 distribution server 6101 according to the present embodiment is connected to internet 6103 and receiving device 6102 according to the present embodiment is connected to LAN6105 and

LAN6105 is connected to internet 6103 through proxy server 6104. Subsequently receiving device 6102 carries out anonymous MPEG4 AV stream communication with MPEG4 distribution server 6101 through LAN6105, proxy server 6104 and internet 6103. Of course it does not matter whether other MPEG4 distribution servers or other types of equipment are connected to internet 6103 and it does not matter whether other receiving devices or other types of equipment are connected to LAN6106.

[0119] Also, in the present embodiment, although the data type is presented as MPEG4, of course other types of data can also be applied to the invention.

[0120] In FIG.23, a variety of devices are devices supporting an IP but since HTTP proxy server 6104 exists between internet 6103 and LAN6105, the IP address on LAN6105 can be a global IP address or a private IP address. Here, the proxy server enters between the internet and the intranet, terminating HTTP once (or other protocols) and concatenating the HTTP sessions at the ends of the proxy server; the proxy server is a server for making possible the distribution of HTTP contents requested by substantial receiving devices (web browser) to distribution servers (WWW server). Note that details on proxy servers are published at for example http://squid.nlanr.net/Squid and elsewhere. In the present embodiment, the MPEG4 distribution server may be a WWW server and the receiving device may be a web browser.

[0121] An example of the authentication procedure and the exchange of authentication keys or the sequence of encrypted data and so on is shown in FIG.24. Since proxy server 6102 enters between receiving device 6102 and MPEG4 distribution server 6101, the relay of actual messages (transmitted as HTTP messages) at proxy server 6102 is the only point that differs from embodiments one through six (FIG.2), the other points of the procedure are the same as in embodiments one through six.

[0122] In the case where formats dependent on the transport protocol such as MPEG4 distribution server 6101, receiving device 6102 and the packet format, corresponding with the above embodiments one through six are adjusted to correspond to the HTTP protocol, formats which correspond to the HTTP protocol such as MPEG4 distribution server 6101, receiving device 6102, the packet format and so on which correspond to the HTTP protocol can be constructed. Below, a structure is presented which corresponds to the structure (see the second embodiment) that attaches an "encryption expansion header" as an expansion header and installs an "MPEG4 expansion header" as a payload header in the payload.

[0123] An example of the interior structure of the MPEG4 distribution server 6101 is shown in FIG.25.

[0124] As shown in FIG.25, the MPEG4 distribution server 6101 in the present embodiment comprises an MPEG4 data generation unit 6301, data encryption unit 6302, MPEG4 payload header attachment unit 6305, HTTP processing unit 6303 which includes encryption header attachment unit 6304 and MIME header attachment unit 6306; TCP/IP and UDP/IP processing unit 6308, link/physical layer processing unit 6309 and authentication/key exchange unit 6311.

[0125] In FIG.24, processes related to sequence authentication and encryption (S6201-S6205) as well as processes related to encryption key updates are performed by authentication/key exchange processing unit 6311.

[0126] HTTP processing unit 6303 corresponds to the RTP processing unit in the present embodiments hitherto and MIME header attachment unit 6306 corresponds to the RTP base header attachment unit in the embodiments hitherto.

[0127] In FIG.26, the IP packet transferred over the internet (and LAN) is shown and in FIG.27, the specifics of the MIME base header and the encryption expansion header are shown.

[0128] In the present embodiment, the encryption expansion header is transferred as one part of MIME. For this reason, information indicating that the encryption expansion header is an encryption expansion header is recorded in the MIME "Content-Type". Also, the MPEG4 expansion header and the MPEG4 data, encrypted as a payload header, are transferred together as one part of MIME. Information is recorded in the "Content-Type" of the MIME indicating that the encrypted MPEG4 data attached to the MPEG4 expansion header is encrypted MPEG4 data. Note that the MIME specifics are disclosed in for example, RFC2045 and so on.

[0129] The format of the encryption expansion header is the same as the first embodiment.

[0130] The internal structure of receiving device 6102 is shown in FIG.28.

[0131] As shown in FIG.28, the MPEG4 distribution server 6101 in the present embodiment comprises link/physical layer processing unit 6701, TCP/IP and UDP/IP processing unit 6702, HTTP processing unit 6703 which includes MIME header analysis unit 6704 and encryption header analysis unit 6706, MPEG4 payload header analysis unit 6705, data encryption-decryption unit 6707, MPEG4 data decoding unit 6708 and authentication/key exchange processing unit 6711.

[0132] In FIG.24, the processes related to sequence authentication and encryption

(the process from S6201–S6205) as well as processes related to encryption key updating are performed by authentication/key exchange processing unit 6711.

[0133] HTTP processing unit 6703 corresponds to the RTP processing units in the embodiments hitherto and MIME header analysis unit 6306 corresponds to the RTP base header reception analysis units in the embodiments hitherto.

[0134] In MPEG4 distribution server 6101, an inputted AV input (for example an analog signal) is compressed into MPEG4 data at MPEG4 data generation unit 6301. Likewise, MPEG4 payload header attachment unit 6305 is notified of necessary information from MPEG4 data generation unit 6301.

[0135] Next, data encryption unit 6302 encrypts the MPEG4 data outputted from MPEG4 data generation unit 301. The encryption key used at that time is the time-variable encryption key Kc above. Likewise, encryption header attachment unit 6304 is notified of necessary information from data encryption unit 6302.

[0136] Next, in HTTP processing unit 6303, an encryption expansion header is attached at encryption header attachment unit 6304 and a MIME header is attached at MIME header attachment unit 6036.

[0137] Subsequently, the encrypted MPEG4 data with the attached MIME header is transmitted at TCP/IP and UDP/IP processing unit 6308 by internet 6103 through link/physical layer processing unit 6309 as an IP packet, as in FIG.26.

[0138] In the MIME header analysis unit 6704 in receiving device 6102 it is ascertained that the data received is possibly an encrypted MPEG4 and also that an encryption expansion header is attached as one part of the MIME. Subsequently, the presence or absence of encryption, the encryption format and the presence of absence of an update to the encryption key can be ascertained from the encryption expansion header at encryption header analysis unit 6706. Then like the second embodiment, the encrypted MPEG4 data is decrypted at encryption-decryption unit 6707, the MPEG4 payload header is analyzed at MPEG4 payload header reception analysis unit 6715 (in the same way as the MPEG4 payload header in the embodiments hitherto), and further, the MPEG4 data is decoded at MPEG4 data generation unit 6708 based on the above analysis result, then outputted as AV output (for example, an analog signal).

[0139] Note that a structure was shown here which attached the "encryption expansion header" as an expansion header and installed the "MPEG4 expansion header" as a payload header but for example, a structure that attaches an "encryption expansion header" and an "MPEG4 expansion header" as expansion headers, and a structure that installs an "encryption expansion header" and an

"MPEG4 expansion header" to a payload as a payload header, are also possible.

[0140] Incidentally, in the embodiments one through seven, in order to notify the receiving side from the transmitting side of an update to the value of Nc as a result of the generation of encryption key Kc, the Even/Odd field of the encryption expansion header (encryption payload header) was used, but instead the Nc value may be transmitted. In this case, the value of Nc is not incremented one by one and can be set to generate randomly for each occasion. Likewise, the Nc value can be changed for each packet.

[0141] Also, RTP and HTTP were utilized as transmission protocol in embodiments one through seven, but of course other protocols may also be utilized. The present embodiments are also not limited to the networks and internets to which it can be applied. Also, as mentioned above, the invention is not limited to the type of data nor an MPEG4 transferred.

[0142] Likewise, data encryption unit 302 and data encryption-decryption unit 707 were installed on the outside of RTP processing units 303 and 307, however they may also be installed on the inside of RTP processing units 303 and 307.

[0143] (Eighth embodiment) Next, the eighth embodiment will be presented.

[0144] In the first through seventh embodiments, the sequence shown in FIG.2 was utilized and the embodiment presented, however the present invention can of course be applied to other sequences.

[0145] Below, an example will be presented utilizing another sequence. Note that the receiving device here may accumulate MPEG4 data distributed by the MPEG4 distribution server.

[0146] The information distribution system in the present embodiment is the same as in FIG.1. In FIG.1, MPEG4 distribution server 101 in the present embodiment and receiving device 102 are connected by internet 103, and a confidential communication of the MPEG4 AV stream is carried out between MPEG4 distribution server 101 and receiving device 102, through internet 103. Of course, it does not matter in the case where other MPEG4 distribution servers and receiving devices or other types of equipment are connected to internet 103.

[0147] Of course, although the data type in the present embodiment is taken to be MPEG4, the present invention can be applied to other types of data.

[0148] The MPEG4 distribution server 101 performs a distribution of MPEG4 data to receiving device 102. The MPEG4 data takes the form of stream distribution and does not take the form of file transmission. Then the MPEG4 data targeted for copyright protection is distributed in an encrypted state. The authentication

procedure and the authentication key exchange procedure is performed at that time before distribution, between MPEG4 distribution server 101 and receiving device 102.

[0149] An example of the sequence for this time is shown in FIG. 29.

[0150] Note that FIG.29 is an illustration of the encryption and authentication of what is called a contents layer; security in layers such as the IP layer or the transport layer, as well as an authentication procedure and so on for these layers, are omitted. Likewise, procedures such as accounting which are performed with priority in the contents layer are also omitted (there may be cases where the accounting process and the authentication/encryption process are not performed).

[0151] Like in the first embodiment, MPEG4 distribution server 101 and receiving device 102 perform authentication and the exchange of certificates (device certification) (S7201, S7202).

[0152] Here, MPEG4 distribution 101 must notify receiving device 102 of encryption key Kc for decrypting contents (AV data that is transmitted) and the measures below are adopted so that an unlimited, unlawful copying of contents at receiving device 102 cannot be performed. In other words, when recording onto a storage media of receiving device 102 (for example DVD-RAM), the AV data is recorded in an encrypted state. Likewise, when data on a storage media is played back, it is confirmed that the data is something recorded onto the storage media originally and in the case where it is not the originally recorded data, playback is disabled. In other words when a copy is made (digital dubbing) from a storage media to another storage media in this case, (for example another DVD-RAM) the copied media will be rendered incapable of playback.

[0153] To this end, MPEG4 distribution server 101 is notified from receiving device 102 of a storage media ID (pass number) MID used in receiving device 102 (step S7203), the encryption key Kc is encrypted in the MPEG4 distribution server using this MID value, and receiving device 102 is notified (step S7204). More specifically, using the pre-determined function g, an encryption key W is generated in the form W=g (MID), the encryption key Kc is encrypted using encryption key W (this encryption key Kc, encrypted by encryption key W, is described as [Kc]w) and [Kc]w is transmitted. Here, the value of MID is taken to be a value that varies by each storage media and is held in sectors which cannot be written to such as ROM.

[0154] Receiving device 102 which has received the above-mentioned [Kc] w utilizes MPEG4 distribution server 101's function g, generates the encryption key W in the form W=g (MID); and using this encryption key W, decrypts [Kc]w and requests encryption key Kc.

[0155] Afterwards, MPEG4 data is generated from the AV data and this MPEG4 data is encrypted by encryption key Kc as above by shared encryption key Kc; the encrypted MPEG4 data is transmitted to receiving device 102 by the AV data (step 7206).

[0156] Meanwhile, receiving device 102 decrypts the encrypted MPEG4 data received as above with the requested encryption key Kc, decodes the relevant MPEG4 data and outputs the data as AV output.

[0157] Also, in the present embodiment, after receiving device 102 accumulates simultaneously or temporarily the AV data it receives(MPEG4 data encrypted by encryption key Kc), it has the function to record the received AV data in the form of MPEG4 data encrypted by encryption key Kc onto a storage media which has the previous MID along with the value of [Kc]w.

[0158] In this case, a device (which could be receiving device 102 or another device) that plays the AV data which was recorded onto the appropriate storage media (MPEG4 data encrypted by encryption key Kc), first reads the values of [Kc]w and MID from the relevant storage media, then generates an encryption key W in the form of W=g (MID); and using this encryption key W the device decrypts [Kc]w and requests encryption key Kc. Subsequently, the device reads the AV data recorded onto the storage media (MPEG4 data encrypted by encryption key Kc) and decodes the MPEG4 data after decrypting the AV data using encryption key Kc.

[0159] On the other hand in the case where an AV data, (MPEG4 data encrypted by encryption key Kc) recorded onto a storage media that has a certain MID1, is copied onto a storage media with a varying MID2, a W cannot be generated since the MID of the original legitimate storage media cannot be derived for a device that plays back the data which recorded on the storage media copied to; and therefore a decryption key Kc cannot be requested from the recorded [Kc] w; and as a result, the recorded encrypted data will be unable to be decrypted. In other words, assuming that the legitimate K, c, W and [Kc]w values to be Kc1, W1=g (MID1) and [Kc] w1, the MID read from the storage media will be MID2, and since encryption key W, which takes MID2 as its basis, becomes W2=g (MID2), the [Kc]w1 read from the relevant storage media is decrypted with W2 and a value different from Kc is calculated (this is taken to be Kc'). Accordingly, even in the case where data [Data] Kc, encrypted with Kc, is decrypted with Kc' , data varying from the original data will be generated and the original data cannot be acquired.

[0160] In this way, even in the case where the AV data received (MPEG4 data encrypted by encryption key Kc) is copied to other storage media, since the MID value

of that storage media differs, the AV data in question can be made incapable of playback and unlawful facsimiles can be prevented.

[0161] Note that, in the present embodiment, the RTP header, the encryption (payload) header and the MPEG4 expansion (payload) header may have the same structures as embodiments one through seven.

[0162] Although MPEG4 was presented as an example of an encoding format in each embodiment above, other encoding methods of course may also be used. For other encoding methods, the constituent elements in question (for example, an MPEG4 data generation unit, an MPEG4 expansion header attachment unit, an MPEG4 data decoding unit, an MPEG4 expansion header reception analysis unit and so on), the expansion header (an MPEG4 expansion header, an MPEG4 payload header), the description of payload type and so on may be modified according to the various encoding methods. Additionally, it is also possible to set the distribution server in each of the embodiments to transmit contents unencrypted. In other words, according to the presence or absence of encryption, the descriptive contents of the with-or-without encryption field, the payload type and so on may be determined at discretion. On the receiving device side as well, the decryption process may be controlled according to the presence or absence of encryption by checking for the presence or absence of encryption in the packet header received.

[0163] Note that it is possible for each function above to be implemented as software.

[0164] Also, the present embodiment may also be implemented as a recording media capable of reading from a computer, which has recorded programs for implementing a given unit (or for making a computer operate as a given unit or for making a computer implement a given function).

[0165] It is possible to realize the present invention in different forms in the technological field not limited to the embodiments mentioned above.

[0166]

[Effects of the invention] With the present invention, it will become possible to expand copy protection not only to IEEE1394, but also to content circulation on the internet and other networks.